DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
WASHINGTON, D.C. 20350-1000

w/ch 4

SECNAVINST 5239.3
NISMC
14 JULY 1995

SECNAV INSTRUCTION 5239.3

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY INFORMATION SYSTEMS SECURITY (INFOSEC) PROGRAM

Ref:
(a) DODD TS3600.1 of 21 Dec 92, Information Warfare (NOTAL)
(b) P.L. 100-235 of 8 Jan 88, Computer Security Act of 1987
(c) OMB Circular A-130 of 15 Jul 94, Management of Federal Information Resources (NOTAL)
(d) NSTISSID No. 500 of 25 Feb 93, Telecommunications and Automated Systems Security Education, Training and Awareness
(e) NSTISSD No. 501 of 16 Nov 92, National Training Program for Information System Security (INFOSEC) Professionals
(f) NSTISSD No. 502 of 5 Feb 93, National Security Telecommunications and Automated Information Security
(g) NSTISSP No. 6 of 8 Apr 94, National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems, (NOTAL)
(h) DODD 5200.28 of 21 Mar 88, Security Requirements for Automated Information Systems (AISs) (NOTAL)
(i) DODD C-5200.5 of 21 Apr 90, Communication Security (COMSEC) (NOTAL)
(j) DODD C-5200.19 of 23 Feb 90, Control of Compromising Emanations (NOTAL)
(k) DODD 5000.2 of 23 Feb 91, Defense Acquisition Policies and Procedure (NOTAL)
(l) CJCSI 6510.01 of 1 Sep 93, Chairman of the Joint Chiefs of Staff Instruction, Joint and Combined Communications Security (NOTAL)
(m) NSTISSI 4009 of 5 Jun 92, National Information Systems Security (INFOSEC) Glossary (NOTAL)
(n) SECNAVINST 5000.2A of 9 Dec 92, Implementation of Defense Acquisition Management Policies, Procedures, Documentation, and Reports (NOTAL)
(o) SECNAVINST 5231.1C of 10 Jul 93, Life Cycle Management Policy and Approval Requirements for Information System Projects
(p) SECNAVINST 5200.32A of 3 May 93, Acquisition Management Policies and Procedures for Computer Resources

Encl:
(1) List of Acronyms
(2) Glossary of Terms

1. Purpose. Emerging as an overarching strategy, the discipline of Information Warfare (IW), as promulgated by reference (a), encompasses not only actions that may be taken to potentially affect an adversary's information or information systems but also addresses those defensive aspects necessary to ensure that U.S. information or information systems are protected against attack. Under this defensive portion of IW, Information Systems Security (INFOSEC) is a subset of information assurance which addresses actions taken to protect U.S. information and information systems. The Department of the Navy (DON) INFOSEC policy and procedures, when properly applied, will be a major component of the efforts necessary to ensure the defense of DON information and information systems. The purpose of this instruction is:

a. To establish DON policy for the INFOSEC Program within the IW discipline and to define the organizational responsibilities for implementation of the security disciplines of Communications Security (COMSEC), Computer Security (COMPUSEC), and Emanations Security (TEMPEST) per references (a) through (l).

b. To provide the basic policy and guidelines necessary for consistent and effective application of resources in ensuring the security of national security systems as well as the security and privacy of DON systems/information under the Computer Security Act of 1987 (reference (b)).

2. Cancellation. SECNAVINST 5239.2.

3. Definitions. Reference (m) contains the official glossary of INFOSEC terms. Additional terms and acronyms relevant to this instruction are contained in enclosures (1) and (2).

4. Objectives

a. To establish a DON INFOSEC program that addresses the defensive aspects of IW as promulgated by reference (a).

b. To ensure that information processed, stored or transmitted by DON information systems is adequately protected with respect to confidentiality, integrity, availability and privacy.

c. To integrate the technical and management processes of the various security disciplines (COMSEC, COMPUSEC, and TEMPEST) into a cohesive INFOSEC program.

d. To establish and implement programs that mandate the certification and accreditation of information systems under DON control.

e. To require a life cycle management approach to implementing INFOSEC requirements.

f. To establish standardized INFOSEC training within the DON.

5. Scope

a. This instruction applies to:

(1) All DON activities.

(2) All DON-sponsored contractors who own, procure, use, operate, or maintain information systems at government or contractor facilities.

(3) All information systems and other system resources designed, developed, procured, or managed by DON activities; and by their contractors.

(4) Information systems operated, but not owned, by DON (e.g., Joint Staff, Department of Defense (DoD)).

b. This instruction applies to the protection of all elements of the information systems. Of all the elements, COMSEC, COMPUSEC, and TEMPEST are managed per this instruction. The other Information Security activities, such as protection of information against accidents, disasters, human error, physical, personnel, and operational security are managed under separate instructions.

6. Background. The DON has recognized the urgent need to integrate all available security capabilities into an unified system-oriented engineering approach to provide responsive, cost effective security measures for our information systems. The DON also recognizes that a thorough and consistent approach to INFOSEC for the protection of our information systems is key to the accomplishment of our defense mission and to the protection of lives, property and technology. Mission and organizational realignments have occurred at multiple levels to ensure an unified approach to DON INFOSEC requirements:

a. INFOSEC Program Implementation: The Chief of Naval Operation (CNO) and the Commandant of the Marine Corps (CMC) have established centralized program development and implementation of the DON INFOSEC Program at their levels.

b. INFOSEC Program Execution: Commander, Space and Naval Warfare Systems Command (COMSPAWARSYSCOM) has created a Program Management organization with DON-wide responsibilities for establishing and executing of an unified system-oriented engineering approach to INFOSEC.

7. Policy

a. Precedence. Policy and requirements set forth by higher authority take precedence over the policy established in this instruction.

b. Fundamental INFOSEC Policy

(1) Data processed, stored and transmitted by information systems shall be adequately protected with respect to requirements for confidentiality, integrity, availability and privacy.

R) (2) All DON information systems shall be protected by the continuous employment of appropriate safeguards.

(3) Classified information processed or stored by DON information systems shall be safeguarded as required by that level of classification.

c. Certification and Accreditation. The appropriate Designated Approving Authority (DAA) shall accredit every DON information system before operation. The accreditation statement shall identify the required confidentiality, integrity, and availability services and constraints under which the system can operate including data sensitivity, user authorization, physical and system configuration. For those information systems supporting cryptologic functions, Sensitive Compartmented Information (SCI)/Intelligence data, or Single Integrated Operations Plan (SIOP) data, accreditation requests shall be forwarded to the appropriate authority.

(1) Certification of DON information systems shall be performed and documented by competent personnel in accordance with specified criteria, standards and guidelines.

(2) Accreditation of DON information systems shall be performed by competent management personnel in a position to balance operational mission requirements and the residual risk of system operation. All accreditation decisions shall be documented and contain a statement of residual risk.

(3) Accreditation of DON information systems shall be performed when information systems are interconnected to other previously accredited information systems and networks. The DAA shall ensure that operation of the resultant system does not incur any additional unacceptable risk.

d. Life Cycle Management. This instruction shall be reviewed for applicability to all DON information systems being acquired in accordance with references (b), (n), (o), and (p). The INFOSEC policy and requirements are applicable throughout the life cycles of all DON systems.

(1) A System Security Plan (SSP) should be developed and maintained for all computer systems (reference (b)). This plan includes the protection strategy planned, including the certification and accreditation processes.

(2) ~~At~~ each milestone decision point, INFOSEC requirements shall be discussed in sufficient detail and tailored to the milestone under review and the complexity of the project. The discussion shall specifically address the issues of confidentiality, integrity and availability.

e. Training. The ability to provide comprehensive assurance that DON information is adequately protected is directly related to the qualifications of the individuals operating DON information systems. In accordance with references (b), (d) and (e) all individuals operating DON information systems will be afforded appropriate training and awareness information commensurate with their duties, responsibilities and the level of information protection required.

8. Responsibilities

a. The Assistant Secretary of the Navy (ASN) for Research, Development, and Acquisition (RD&A) shall:

(1) Issue the appropriate DON policies and guidance providing implementation details and procedures for the INFOSEC program.

(2) Oversee the DON acquisition process as it relates to the INFOSEC program.

b. The Deputy Assistant Secretary of the Navy (DASN) for Command and Control, Communications, Computers, and Intelligence/Electronic Warfare/Space (C4I/EW/Space) shall review resource requirements necessary to implement and execute the DON INFOSEC program.

c. The Commander, Naval Information Systems Management Center (NISMC) shall:

(1) Serve as the coordinator for DON INFOSEC Policy.

(2) Ensure that INFOSEC activities, with respect to the scope of programs covered by reference (p), are integrated into the overall DON major system acquisition process.

(3) Ensure that INFOSEC is integrated into the DON Life Cycle Management process.

(4) Monitor the implementation of this instruction.

d. The Chief of Naval Operations (CNO) shall:

(1) Serve as the Program/Resource Sponsor for the DON INFOSEC Program.

(2) Manage the Navy INFOSEC Program including DON program development, implementation, planning, programming, and budgeting.

(3) Establish and validate Navy INFOSEC requirements; coordinate INFOSEC requirements of joint military department concern with the Joint Staff in accordance with reference (k).

(4) Establish senior INFOSEC advisory boards with CMC representation to advise on DON INFOSEC policy and guidance as required.

(5) Coordinate the development and implementation of appropriate guidance documents.

(6) Provide Navy representative to the National Security Telecommunications and Information System Security Committee (NSTISSC), Subcommittee for Telecommunications Security (STS), and Subcommittee for Information System Security (SISS).

(7) Serve as the DAA for Navy-wide and joint service information systems (where Navy is the assigned lead) and ensure that DAAs are identified for other Navy information systems.

(8) Advise NISMC of INFOSEC issues that may have a DON or DoD-wide impact.

(9) Develop a DON INFOSEC training program.

(10) Develop and maintain the DON INFOSEC Master Plan in coordination with CMC and Systems Commands.

(11) Coordinate DON INFOSEC requirements for the DON Service Cryptologic Element (SCE) security program with the National Security Agency (NSA).

(12) Coordinate DON INFOSEC requirements for the DON Sensitive Compartmented Information (SCI)/Intelligence program, and the DON portion of the DoD Intelligence Information System (DODIIS) with the Defense Intelligence Agency (DIA).

(13) Provide recommendations to NISMC for the revision of other DoD and DON documents to standardize DON INFOSEC across all activities.

e. The Commandant of the Marine Corps (CMC) shall:

(1) Advise NISMC of Marine Corps INFOSEC issues that may have a DON or DoD-wide impact.

(2) Ensure that DAAs are identified and security services provided for Marine Corps information systems.

(3) Endorse and forward Marine Corps validated INFOSEC software and equipment procurement requirements to CNO for equal consideration during the development of the DON Program Objective Memorandum (POM).

(4) Submit validated Marine Corps INFOSEC requirements to CNO for inclusion in the DON INFOSEC Master Plan.

(5) Establish senior INFOSEC advisory boards with CNO to advise on DON INFOSEC policy and guidance as required.

(6) Provide recommendations to NISMC for the revision of other DoD and DON documents to institutionalize INFOSEC.

(7) Provide CMC representation to the NSTISSC, STS, and SISS.

f. The Chief of Naval Research (CNR) shall:

(1) Manage the DON INFOSEC Program within the Office of Naval Research (ONR).

(2) Advise NISMC of ONR INFOSEC issues that may have a DON or DoD-wide impact.

(3) Provide appropriate representation to INFOSEC advisory boards.

(4) Ensure that a DAA and security support are provided for each ONR information system.

(5) Consolidate and forward the ONR COMSEC equipment requirements to CNO for validation and consideration during development of the POM.

(6) Provide the technical base for the DON INFOSEC Research and Development (R&D) Program within ONR.

(7) Designate a DON Center for Computer High Assurance Systems (CCHAS). As part of the DON INFOSEC Program, the CCHAS shall:

(a) Maintain liaison with NSA regarding INFOSEC R&D.

(b) Conduct R&D in evaluation methodologies for application systems.

(c) Provide INFOSEC research support to other DON activities.

g. The Commanders, Naval Systems Commands (SYSCOMs) shall:

(1) Submit INFOSEC POM recommendations to CNO for validation and consolidation in the DON INFOSEC Master Plan. Marine Corps recommendations shall be submitted via CMC.

(2) Coordinate INFOSEC integration into information systems with COMSPAWARSYSCOM.

(3) Ensure that each information system acquisition or deployment under the command's purview adheres to the DON life cycle management policy.

h. Commander, Space and Naval Warfare Systems Command (COMSPAWARSYSCOM). In addition to the responsibilities set forth for SYSCOMs, COMSPAWARSYSCOM shall:

(1) As the technical lead for DON INFOSEC, provide systems engineering and integration support to the systems commands for all DON information systems with INFOSEC requirements.

(2) Budget for DON INFOSEC programs as defined in the INFOSEC Master Plan.

(3) Integrate INFOSEC engineering and integration into the Warfare Systems Engineering Process.

(4) Develop and manage the DON INFOSEC R&D Program.

(5) Develop and acquire DON standard and specified INFOSEC products in accordance with the DON INFOSEC Master Plan, ensuring that a Certification Authority and an In-Service Engineering Activity (ISEA) and/or Software Support Activity (SSA) are assigned.

(6) Budget for operations and maintenance funding for fielded DON centrally procured INFOSEC products and systems throughout their life-cycle.

(7) Establish Memorandum of Agreement (MOA) with NSA, as necessary, to facilitate the embedding and/or development of INFOSEC equipment/models.

(8) Provide direct liaison with NISMC on INFOSEC acquisition issues.

i. The Director, Naval Criminal Investigative Service (NCIS) shall:

(1) Investigate fraud, waste, abuse and other criminal violations involving DON information systems.

(2) Maintain a staff skilled in the investigation of computer crime. This staff may be augmented, when necessary, by personnel provided by other DON activities.

(3) Collect threat information and disseminate as appropriate.

9. Action. All action addressees shall implement this guidance within their organizations. All developing and operating activities shall budget for, fund and execute the actions necessary to comply with this instruction and the implementing documents that support it.

W. C. Bowes
Principal Deputy Assistant
Secretary of the Navy (Research,
Development and Acquisition)

Distribution:

SNDL	A1	(Immediate Office of the Secretary)
		(AAUSN, ASN(RDA) and DASN (C4I/EW/Space) only)
	A2A	(Department of the Navy Staff Offices) (CNR and NAVCOMPT only)
	A3	(Chief of Naval Operations) (N6 and N09 only) (25)
	A6	(CMC) (75)
	D30	(NAVINFOSYSMGTCEN) (50)
	FKA1	(Syscoms Commands)
	MARCORPS PCN 71000000000 and 71000000100	

Copy to:

SNDL	22A	(Fleet Commanders)
	24	(Type Commanders) (less 24E)
	26H	(Fleet Training Group and Detachment)
	A2A	(Department of the Navy Staff Offices) (less CNR and NAVCOMPT)
	B1B	(Offices of the Secretary of Defense)
	B3	(College and University)
	B5	(U. S. Coast Guard)
	C25A	(OPNAV Support Activity Detachment (Ft. Ritchie, only))
	C4L	(Navy Laboratories)

Copy to: (Continued)

SNDL	C4EE	(Center for Naval Analyses)
	FKP14	(FCDSSA)
	FKP16	(NAVSSES)
	FKP18	(NAVSEAADSA)
	FKP20	(AEGIS TRACEN)
	FL4	(Regional Data Automation Center, Data Automation Facility)
	FT74	(NROTCU)
	W	(Department of the Navy Echelon 2 Activities) (less Syscoms) (5)

SECNAV/OPNAV Directives Control Office
Washington Navy Yard Building 200
901 M Street SE
Washington, DC 20374-5074 (20 copies)

Order from:
Naval Inventory Control Point
Cog "I" Material
700 Robbins Avenue
Philadelphia, PA 19111-5098

Stocked: 50 copies

LIST OF ACRONYMS

AIS	Automated Information Systems
ASN	Assistant Secretary of the Navy
CCHAS	Center for Computer High Assurance Systems
CMC	Commandant of the Marine Corps
COMPUSEC	Computer Security
COMSEC	Communications Security
CNO	Chief of Naval Operations
CNR	Chief of Naval Research
DAA	Designated Approving Authority
DASN (C4I/EW/Space)	Deputy Assistant Secretary of the Navy (Command, Control, Communications, Computers and Intelligence/Electronic Warfare/Space)
DIA	Defense Intelligence Agency
DoD	Department of Defense
DODIIS	Department of Defense Intelligence Information System
DON	Department of the Navy
INFOSEC	Information Systems Security
IS	Information System
ISEA	In-Service Engineering Activity
IW	Information Warfare
LCM	Life Cycle Management
MARCORSYSCOM	Marine Corps Systems Command
MOA	Memorandum of Agreement
NCIS	Naval Criminal Investigative Service
NISMC	Naval Information Systems Management Center
NSA	National Security Agency
NSTISSC	National Security Telecommunications and Information System Security Committee
ONR	Office of Naval Research
POM	Program Objective Memorandum
RD&A	Research, Development and Acquisition
R&D	Research and Development
SCI	Sensitive Compartmented Information
SECNAV	Secretary of the Navy
SIOP	Single Integrated Operations Plan
SISS	Subcommittee on Information Systems Security
SPAWAR	Space and Naval Warfare Systems Command
SSA	Software Support Activity
SSP	System Security Plan
STS	Subcommittee on Telecommunications Security
SYSCOM	Systems Command

GLOSSARY OF TERMS

Many of the terms used in this instruction are drawn from different specialization areas, and their special meanings in the context of the DON INFOSEC Program may differ from the common English usage. This enclosure explains how such terms are commonly used in the INFOSEC Community.

1. Accreditation. Formal declaration by a Designated Approving Authority (DAA) that an AIS is approved to operate in a particular security mode using a prescribed set of safeguards.

2. Accreditation Authority. Synonymous with designated approving authority (DAA).

3. Assessment. The laboratory and field examination of products, components, or application systems against NSA or service defined criteria for an anticipated operating environment. Assessment involves a thorough examination of security mechanisms but not necessarily all assurances. See *Evaluation*.

4. Availability. The property that ensures the information system's data, services, and resources are available to authorized users reliably, consistently, and in a timely manner.

5. Certification. Comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

6. Certification Authority. The official (e.g., Program Manager, etc) responsible for an information system's certification process and the signature authority for the certification statement.

7. Communications Security (COMSEC). Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. NOTE: Communications security includes crypto security, transmission security, emission security, and physical security of COMSEC material.

8. Computer Security (COMPUSEC). Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

9. Critical. Relating to information system data, services, or other resources whose availability is necessary for successful execution of the DON mission supported by the information system.

10. Data. Text, video, audio, imagery, and telemetry used as information or in control functions in an information system. For this instruction, data may reside in any form or media, including human and machine readable, such as magnetic disk and tape, optical disk, paper, punch cards, paper tape, video displays, audio forms, electrical signals, radio-frequency signals, and optical signals. See *Information*.

11. Designated Approving Authority (DAA). Official with the authority to formally assume the responsibility for operating an AIS or network at an acceptable level of risk.

12. Evaluation. The examination of products or components against defined criteria. Evaluation has three forms: trusted product evaluation, in which products or components are evaluated against a specified class of the Trusted Computer System Evaluation Criteria or its interpretations; cryptographic product evaluation, in which products or components are evaluated to provide appropriate cryptographic mechanisms; and TEMPEST product evaluation, in which products are evaluated to meet national standards for emissions security.

13. Firmware. Equipments or devices within which computer programming instructions necessary to the performance of the device's discrete functions are electrically embedded in such a manner that they cannot be electrically altered during normal device operations.

14. Hardware. The electric, electronic, and mechanical equipment used for processing data

15. Information. The meaning assigned to data based on the data's representation. See *Data*.

16. Information System (IS). Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.

17. Information Systems Security (INFOSEC). The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

18. INFOSEC Master Plan. The INFOSEC Master Plan describes the current DON INFOSEC baseline and threats; projects INFOSEC requirements and threats into the future; analyzes potential sources for meeting those requirements; and prioritizes SPAWAR INFOSEC investments to lower DON INFOSEC risks.

19. Integrity. The security property that ensures that data is not modified by unauthorized users, services, or components or that ensures a critical process cannot be affected by unauthorized interaction.

20. National Security Systems. Telecommunications and automated information systems operated by the U.S. Government, its contractors, or its agents, that contain classified information or, as set forth in 10 U.S.C. Section 2315, that involves intelligence activities, involves cryptologic activities related to national security, involves command and control of military forces, involves equipment that is an integral part of a weapon or weapon system, or involves equipment that is critical to the direct fulfillment of military or intelligence missions.

21. Network. A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include Automated Information Systems (AISs), packet switches, telecommunications controllers, key distribution centers, and technical control devices.

22. Personnel Security. The procedures established to ensure that personnel with access to sensitive or classified data, services, and resources have the required investigation, clearances, and access authorizations. In addition, personnel security includes security training and awareness specific to information systems users.

23. Physical Security. The use of barriers, guards, locks, badges and related measures to control physical access to an information system, its resources, and facilities.

24. Risk. A combination of the likelihood that a threat shall occur, the likelihood that a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact.

25. Security Safeguards. The protective measures and controls that are prescribed to meet the security requirements specified for an AIS. These safeguards may include, but are not necessarily limited to, hardware and software security features; operation procedure; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices.

26. Service. An automated capability provided by an information system. For the purposes of this instruction, services can be categorized as data processing services and data transfer services.

27. Software (or Computer Software). A combination of associated computer instructions and computer data definitions required to enable the computer hardware to perform computational or control functions.

28. TEMPEST. Short name referring to investigation, study, and control of compromising emanations from information systems and telecommunications equipment.